Claims

1. A method for accessing encrypted data by a client, the method comprising the steps of:

receiving by a server from a client client information derived from a first secret wherein the client information is derived such that the server can not feasibly determine the first secret;

providing to the client by the server intermediate data, the intermediate data derived responsive to at least the received client information and to a server secret, wherein the intermediate data is derived such that the client can not feasibly determine the server secret;

authenticating the client by a device, the device storing encrypted secrets and configured not to provide the encrypted secrets without authentication; and

after the authenticating step, providing to the client by the device the encrypted secrets, wherein the encrypted secrets are capable of being decrypted using a third secret that is derived from the intermediate data.

2. The method of claim 1 wherein the third secret is derived from the intermediate data by use of one of a key derivation function and a hash function.

3. The method of claim 1 wherein the third secret is the intermediate data.

4. The method of claim 1 wherein the first secret comprises at least one of a PIN, a password, and biometric information.

5. The method of claim 1 wherein the intermediate data is derived from at least the first secret and the server secret by use of a blind function evaluation protocol.

6. The method of claim 5 wherein the security of the blind function evaluation protocol is based on the problem of extracting roots modulo a composite.

7. The method of claim 5 wherein the security of the blind function evaluation protocol uses discrete logarithms.

8. The method of claim 1 wherein the authenticating step comprises authenticating the client based on a time-dependent code.

9. The method of claim 1 wherein the authenticating step comprises authenticating the client based on at least one of a PIN, a password, and biometric information.

10. The method of claim 1 wherein the authenticating step comprises authenticating the client based on a secret other than the first secret.

11. The method of claim 1 wherein the authenticating step comprises using a secret derived from the intermediate data.

12. The method of claim 1 wherein the device comprises at least one of a file server, a directory server, a key server, a PDA, a mobile telephone, a smart card, and a desktop computer.

13. The method of claim 12 wherein the device comprises at least one secure data store, the device requiring authentication before allowing the client access to the data store.

14. The method of claim 1 wherein the encrypted secrets comprise a private key of a public/private key pair used for asymmetric cryptography.

15. The method of claim 14 wherein the encrypted secrets comprise a signature key used for creating a digital signature.

16. The method of claim 15 wherein the authenticating step comprises authenticating the client based on a secret other than the first secret, so that the user provides different information to access the device and access the signature key.

17. The method of claim 1 wherein the encrypted secrets comprise a secret key used for symmetric cryptography.

18. The method of claim 1 wherein the encrypted secrets comprise at least one unit of digital currency.

19. The method of claim 1 further comprising the step of verifying that the client has not exceeded a predetermined number of unsuccessful attempts to obtain the intermediate data.

20. The method of claim 19 wherein the verifying step further comprises:

transmitting a challenge code to the client; and

receiving the result of a cryptographic operation using the challenge code as an input and using a cryptographic key derived from the encrypted secret.

21. A system for accessing encrypted data by a client, the system comprising:

a first server comprising:

a first server receiver for receiving from a client client information derived from a first secret wherein the client information is derived such that the first server can not feasibly determine the first secret;

a first data store storing a server secret; and

a first server output for providing to the client by the first server intermediate data, the intermediate data derived responsive to at least the received client information and to a server secret, wherein the intermediate data is derived such that the client can not feasibly determine the server secret; and

a device, comprising:

a second data store storing an encrypted secret, the encrypted secret capable of being decrypted using a third secret that is derived from the intermediate data;

an authentication subsystem for authenticating the client by the device; and

a device output for providing to the client by the device the encrypted secrets upon authentication.

22. The system of claim 21 wherein the third secret is derived from the intermediate data by use of a key derivation function.

23. The system of claim 21 wherein the intermediate data is derived from at least the first secret and the server secret by use of a blind function evaluation protocol.

24. The system of claim 23 wherein the security of the blind function evaluation protocol is based on the problem of extracting roots modulo a composite.

25. The system of claim 23 wherein the security of the blind function evaluation protocol is based on the principles of discrete logarithms.

26. The system of claim 21 wherein the authentication subsystem authenticates the client based on a secret other than the first secret.

27. The system of claim 21 wherein the authentication subsystem authenticates the client using a secret derived from the intermediate data.

28. The system of claim 21 wherein the second device comprises at least one of a file server, a directory server, a key server, a PDA, a mobile telephone, a smart card, and a desktop computer.

29. The system of claim 21 wherein the encrypted secret comprises at least one secret chosen from the set of a private key of a public/private key pair used for asymmetric cryptography, a signature key used for creating a digital signature, a secret key used for symmetric cryptography, and at least one unit of digital currency.

30. The system of claim 21 wherein the first server further comprises a verifier for verifying that the client has not exceeded a predetermined number of unsuccessful attempts to obtain the intermediate data.

31. A method for decrypting encrypted secrets associated with a client by a network server, the method comprising the steps of:

receiving from a client a first secret;

transmitting client information to a first server, the client information derived from the first secret such that the first server can not feasibly determine the first secret;

receiving from the first server intermediate data, the intermediate data derived responsive to at least the client information and to a first server secret, wherein the intermediate data is derived by the second server such that the server secret cannot feasibly be determined;

deriving a decryption key from the intermediate data; and

decrypting the encrypted secrets using the decryption key.

32. The method of claim 31 wherein the network server is a web server and wherein the client is a web browser.

33. The method of claim 31 wherein the deriving step is performed using a key derivation function.

34. The method of claim 31 wherein the intermediate data is derived using a blind function evaluation protocol.

35. The method of claim 31 wherein the intermediate data is derived using a blind function evaluation protocol.

36. The method of claim 31 wherein the encrypted secrets comprise encrypted personal information associated with a user of the client.

37. A network server for accessing encrypted secrets associated with a client, the method comprising the steps of:

a first receiver for receiving from a client a first secret;

a transmitter for transmitting client information to a first server, the client information derived from the first secret such that the first server can not feasibly determine the first secret;

a second receiver for receiving from the first server intermediate data, the intermediate data derived responsive to at least the client information and to a first server secret, wherein the intermediate data is derived by the second server such that the server secret cannot feasibly be determined;

a key derivation function for deriving a decryption key from the intermediate data; and

a decryption function for decrypting the encrypted secrets using the decryption key.

38. A method for authenticating to a network server, the method comprising the steps of:

transmitting to a first server client information derived from a first secret wherein the client information is derived such that the server can not feasibly determine the first secret;

receiving from the first server intermediate data, the intermediate data derived responsive to at least the received client information and to a server secret, wherein the intermediate data is derived such that the client can not feasibly determine the server secret;

deriving a server password by the client from the intermediate data and a server identifier;

authenticating to the network server using the server password.

39. The method of claim 38 further comprising the step of transmitting to the first server by the network server verification that the user has authenticated successfully.

40. The method of claim 38 wherein the network server is a web server.

41. The method of claim 38 wherein the deriving step comprises deriving a server password using a key derivation function.

42. A system for authenticating to a network server, comprising:

a first transmitter for transmitting to a first server client information derived from a first secret wherein the client information is derived such that the server can not feasibly determine the first secret;

a receiver for receiving from the first server intermediate data, the intermediate data derived responsive to at least the received client information and to a server secret, wherein the intermediate data is derived such that the client can not feasibly determine the server secret;

a key derivation function for deriving a server password by the client from the intermediate data and a server identifier; and

a first transmitter for transmitting the server password to the network server to authenticate to the network server./